(12) UK Patent Application (19) GB (11) 2 371 639 (13) A

(43) Date of A Publication 31.07.2002

(21) Application No 0101864.7

(22) Date of Filing 24.01.2001

(51) INT CL[7]
G06F 17/60 1/00

(52) UK CL (Edition T)
G4A AAP AUXF

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition S) G4A AAP AUDB AUXF AUXX
INT CL[7] G06F 1/00 17/60
Online: EPODOC, WPI, JAPIO

(71) Applicant(s)
Ling-Chi Li
No 223-5 Fu-Hsin St, Hsin-hua Town, Tainan County, Taiwan

Tsung-Hsin Chang
Flat 7, 22 St. George's Square, LONDON, SW1 2HP, United Kingdom

Hon Shen
18 Pembroke House, Hallfield Estate, LONDON, W2 6HG, United Kingdom

(72) Inventor(s)
Ling-Chi Li
Tsung-Hsin Chang

(74) Agent and/or Address for Service
Marks & Clerk
57-60 Lincoln's Inn Fields, LONDON, WC2A 3LS, United Kingdom

(54) Abstract Title
Secure network payment system

(57) A payment method for making payments over a network 400 comprises setting up (fig 3) a customer account at a payment centre 300; accessing a supply server; receiving a customer order for goods or services at the supply server 500, the customer order comprising payment information identifying the customer account at the payment centre 300; at the supply server 500, transmitting over the network 600 the payment information and information on the value of the goods or services to the payment centre 300; at the payment centre 300, using the payment information to perform a validation check on the customer order by accessing data on the customer's account and responding by sending validation information to the supply server 500; and at the supply server 500, responding to the validation information to process the customer order accordingly; wherein at the payment centre 300 a plurality of validation servers (310,320 fig 2) are provided, each validation server (310,320 fig 2) being controlled to connect one at a time for a period of time to the network 400 to receive the payment information, to perform a validation check, and to send the authorisation information to the supply server 500.

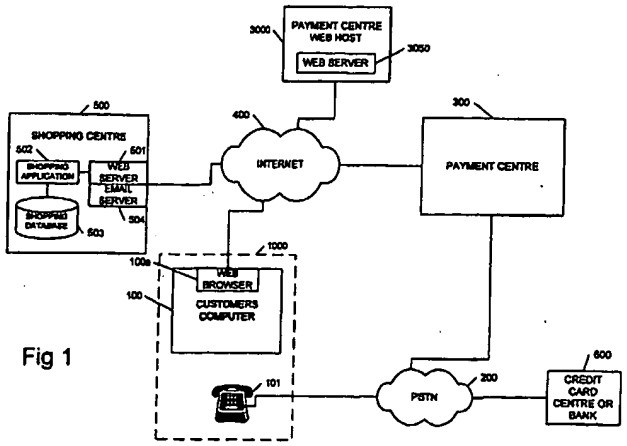


Fig 1

GB 2 371 639 A

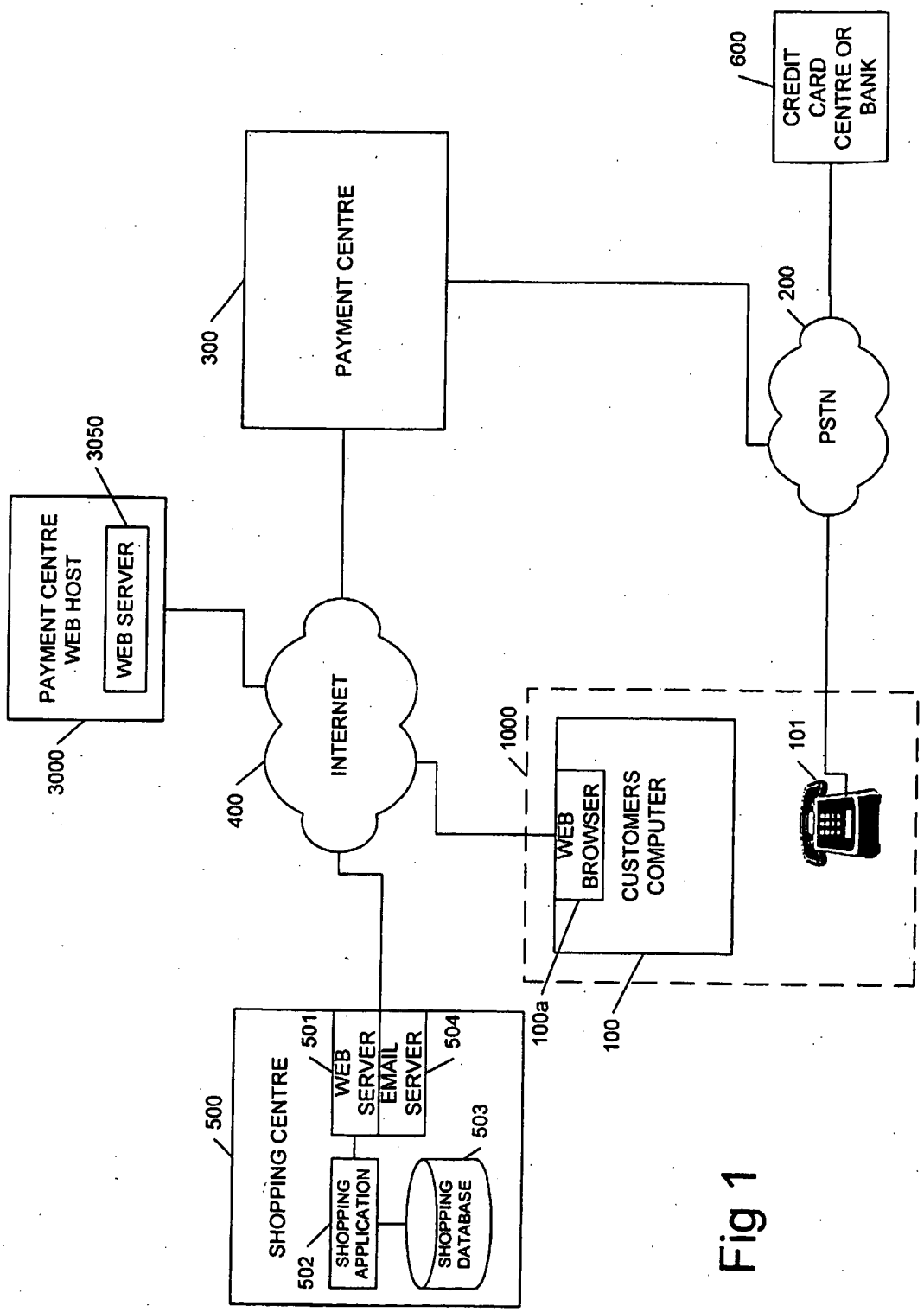

600
CREDIT CARD CENTRE OR BANK
300
PAYMENT CENTRE
200
PSTN
3050
PAYMENT CENTRE WEB HOST
WEB SERVER
3000
400
INTERNET
1000
WEB BROWSER
CUSTOMERS COMPUTER
101
100a
100
500
SHOPPING CENTRE
501
WEB SERVER
504
EMAIL SERVER
503
SHOPPING DATABASE
502
SHOPPING APPLICATION

Fig 1

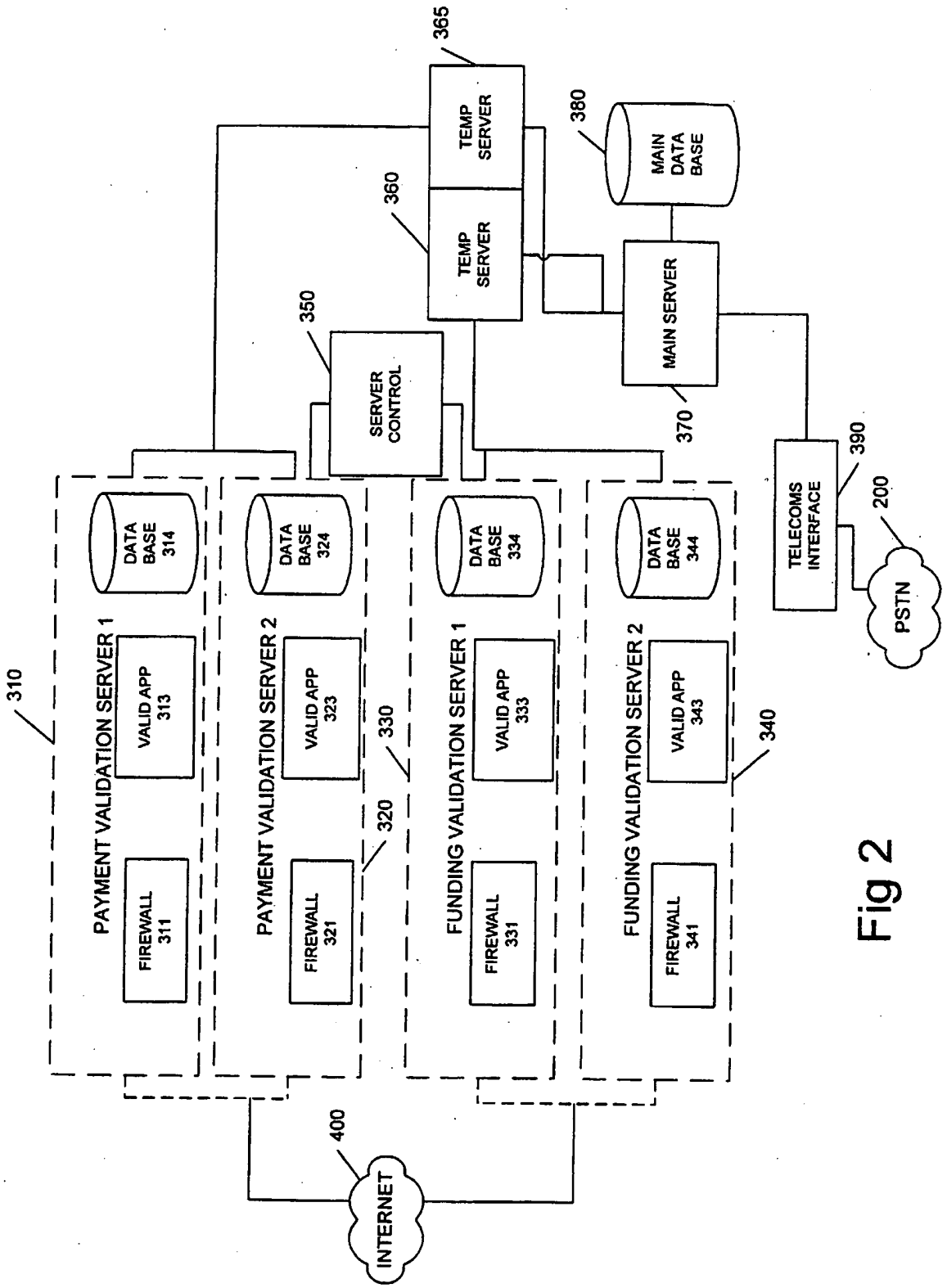

365
TEMP SERVER
380
MAIN DATA BASE
360
TEMP SERVER
MAIN SERVER
350
SERVER CONTROL
370
390
TELECOMS INTERFACE
200
PSTN
DATA BASE 314
DATA BASE 324
DATA BASE 334
DATA BASE 344
310
PAYMENT VALIDATION SERVER 1
VALID APP 313
FIREWALL 311
PAYMENT VALIDATION SERVER 2
VALID APP 323
FIREWALL 321
330
320
FUNDING VALIDATION SERVER 1
VALID APP 333
FIREWALL 331
FUNDING VALIDATION SERVER 2
VALID APP 343
FIREWALL 341
340
400
INTERNET

Fig 2

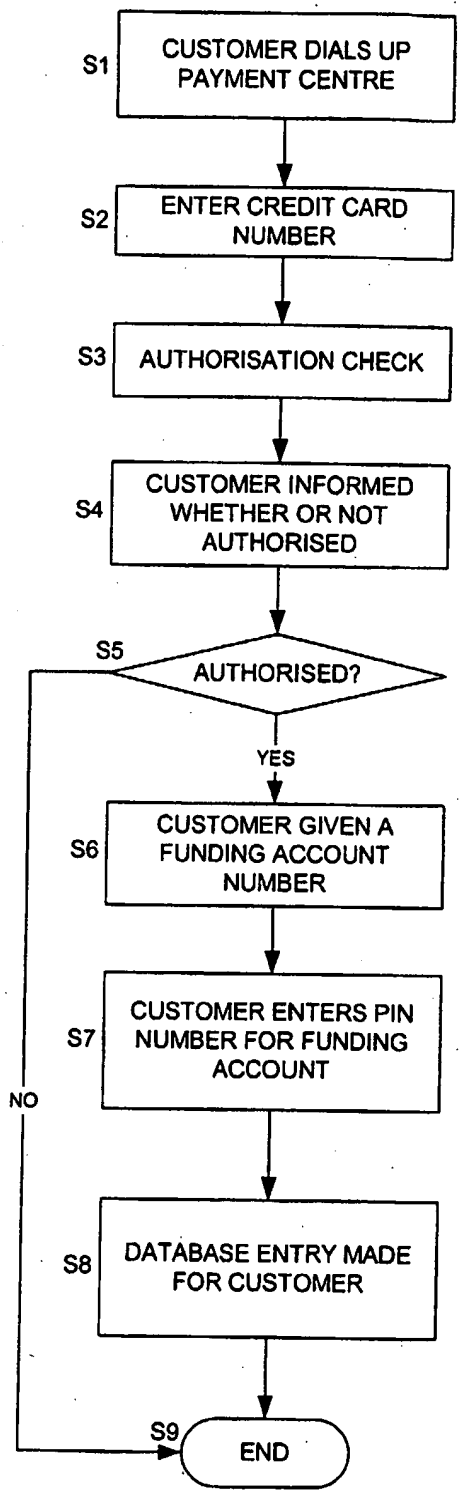

S1
CUSTOMER DIALS UP PAYMENT CENTRE
S2
ENTER CREDIT CARD NUMBER
S3
AUTHORISATION CHECK
S4
CUSTOMER INFORMED WHETHER OR NOT AUTHORISED
S5
AUTHORISED?
YES
NO
S6
CUSTOMER GIVEN A FUNDING ACCOUNT NUMBER
S7
CUSTOMER ENTERS PIN NUMBER FOR FUNDING ACCOUNT
S8
DATABASE ENTRY MADE FOR CUSTOMER
S9
END

Fig 3

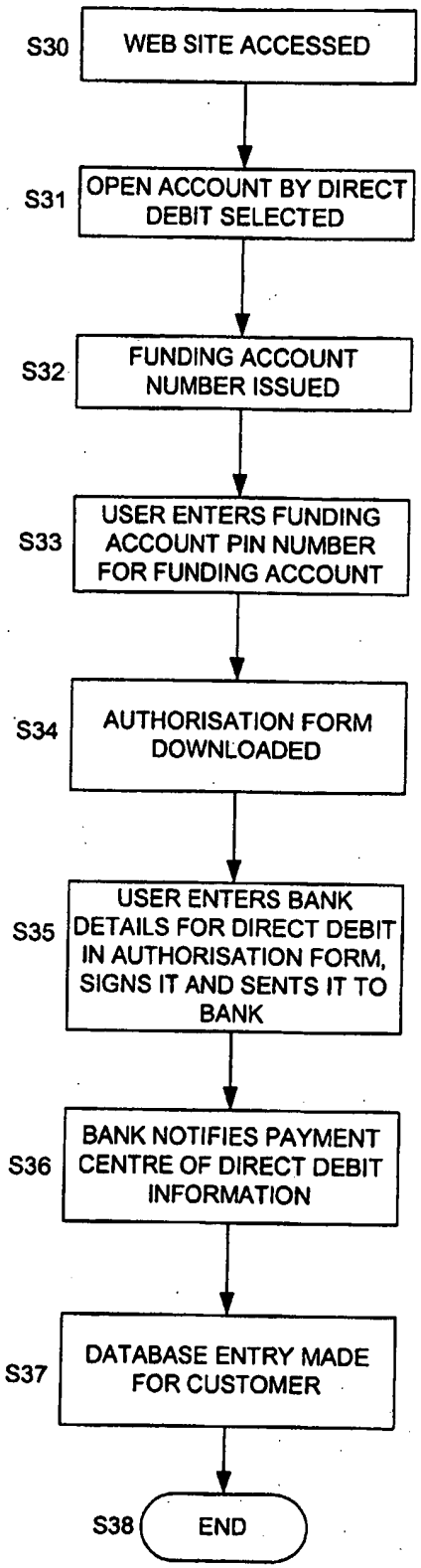

S30
WEB SITE ACCESSED
S31
OPEN ACCOUNT BY DIRECT DEBIT SELECTED
S32
FUNDING ACCOUNT NUMBER ISSUED
S33
USER ENTERS FUNDING ACCOUNT PIN NUMBER FOR FUNDING ACCOUNT
S34
AUTHORISATION FORM DOWNLOADED
S35
USER ENTERS BANK DETAILS FOR DIRECT DEBIT IN AUTHORISATION FORM, SIGNS IT AND SENTS IT TO BANK
S36
BANK NOTIFIES PAYMENT CENTRE OF DIRECT DEBIT INFORMATION
S37
DATABASE ENTRY MADE FOR CUSTOMER
S38
END

Fig 4

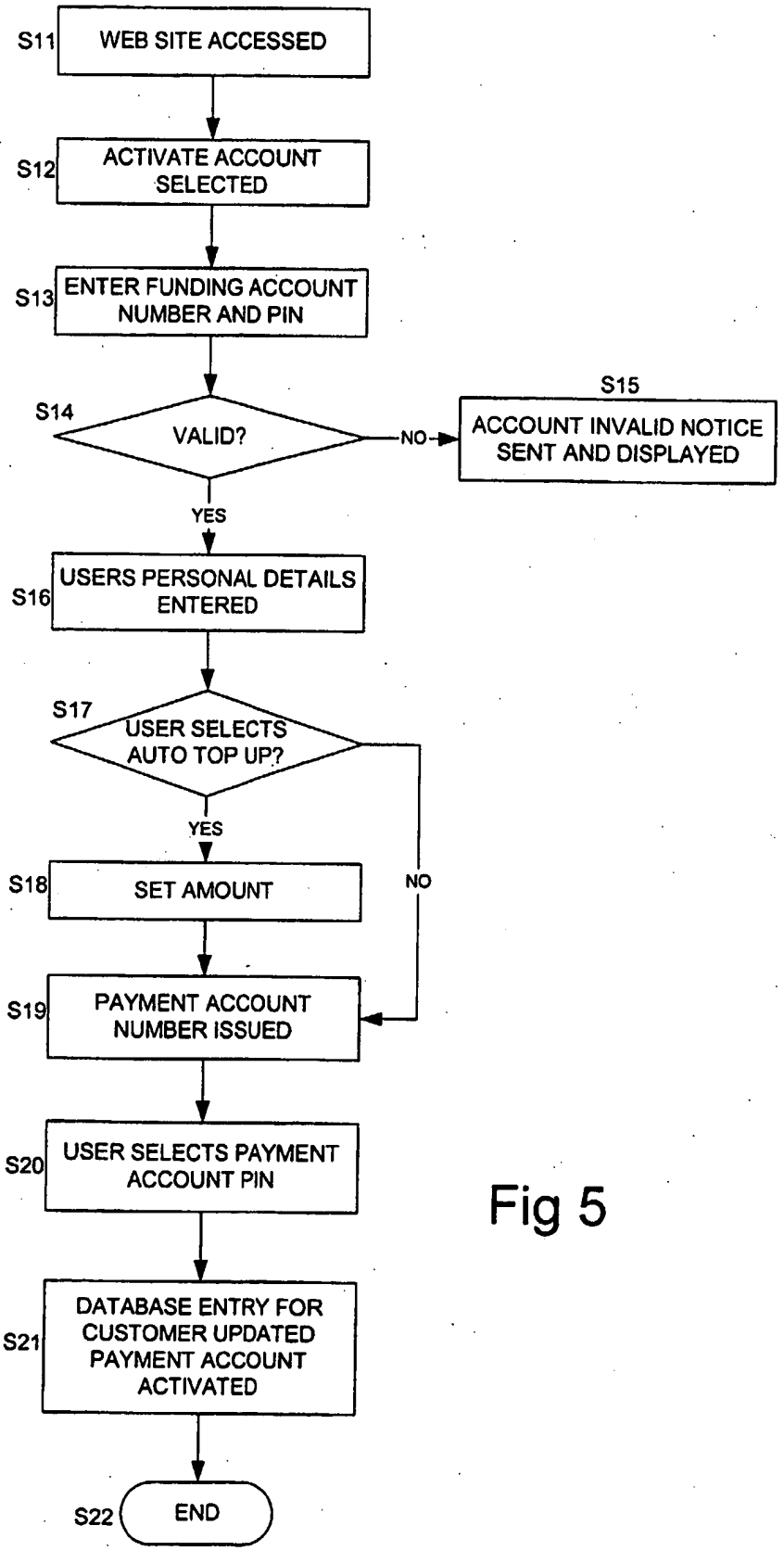
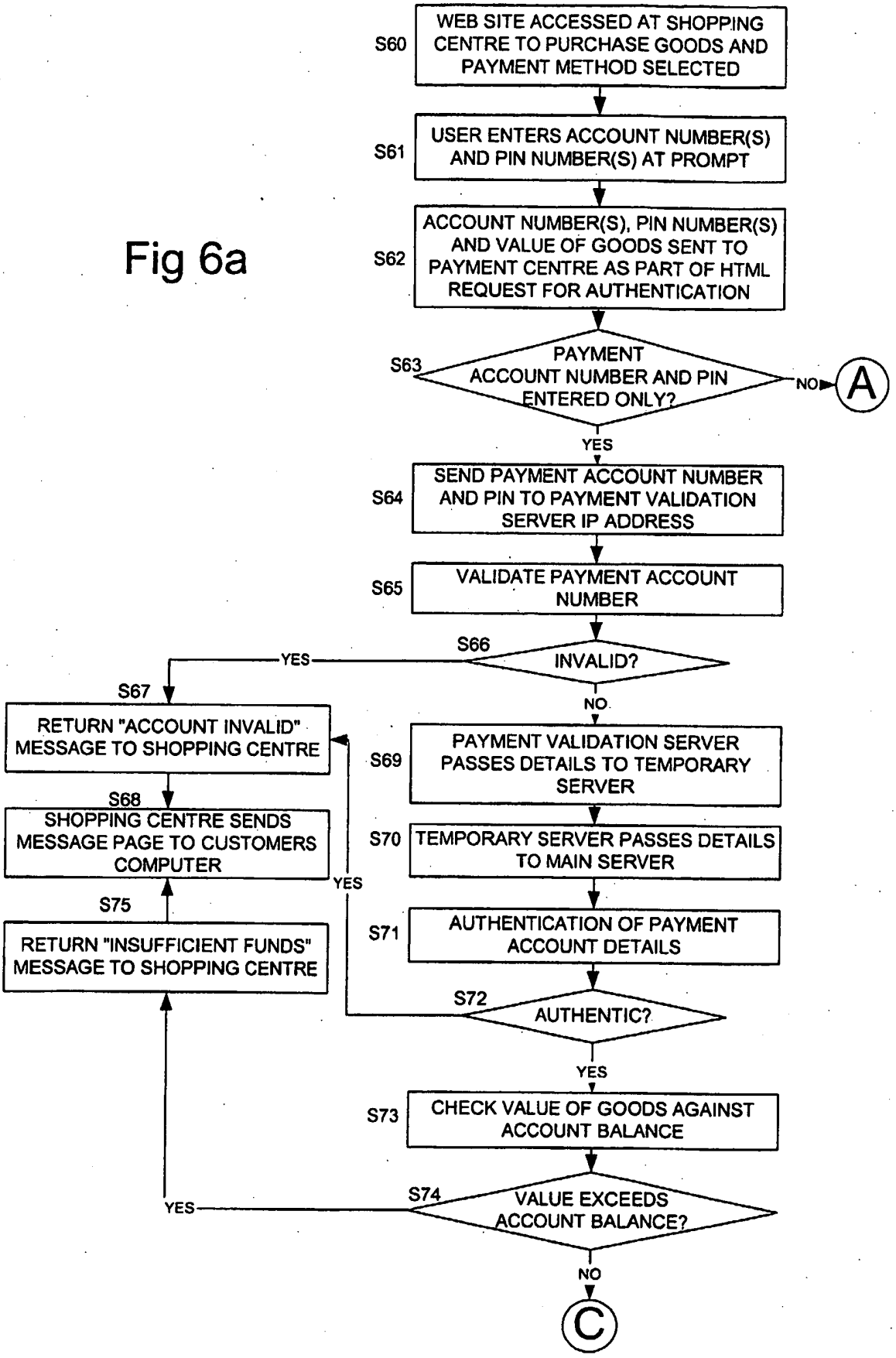

S11
WEB SITE ACCESSED
S12
ACTIVATE ACCOUNT SELECTED
S13
ENTER FUNDING ACCOUNT NUMBER AND PIN
S14
VALID?
NO
S15
ACCOUNT INVALID NOTICE SENT AND DISPLAYED
YES
S16
USERS PERSONAL DETAILS ENTERED
S17
USER SELECTS AUTO TOP UP?
YES
NO
S18
SET AMOUNT
S19
PAYMENT ACCOUNT NUMBER ISSUED
S20
USER SELECTS PAYMENT ACCOUNT PIN
S21
DATABASE ENTRY FOR CUSTOMER UPDATED PAYMENT ACCOUNT ACTIVATED
S22
END

Fig 5

Fig 6a


S60
WEB SITE ACCESSED AT SHOPPING CENTRE TO PURCHASE GOODS AND PAYMENT METHOD SELECTED
S61
USER ENTERS ACCOUNT NUMBER(S) AND PIN NUMBER(S) AT PROMPT
S62
ACCOUNT NUMBER(S), PIN NUMBER(S) AND VALUE OF GOODS SENT TO PAYMENT CENTRE AS PART OF HTML REQUEST FOR AUTHENTICATION
S63
PAYMENT ACCOUNT NUMBER AND PIN ENTERED ONLY?
NO
A
YES
S64
SEND PAYMENT ACCOUNT NUMBER AND PIN TO PAYMENT VALIDATION SERVER IP ADDRESS
S65
VALIDATE PAYMENT ACCOUNT NUMBER
S66
INVALID?
YES
NO
S67
RETURN "ACCOUNT INVALID" MESSAGE TO SHOPPING CENTRE
S68
SHOPPING CENTRE SENDS MESSAGE PAGE TO CUSTOMERS COMPUTER
S75
RETURN "INSUFFICIENT FUNDS" MESSAGE TO SHOPPING CENTRE
S69
PAYMENT VALIDATION SERVER PASSES DETAILS TO TEMPORARY SERVER
S70
TEMPORARY SERVER PASSES DETAILS TO MAIN SERVER
S71
AUTHENTICATION OF PAYMENT ACCOUNT DETAILS
S72
AUTHENTIC?
YES
YES
S73
CHECK VALUE OF GOODS AGAINST ACCOUNT BALANCE
S74
VALUE EXCEEDS ACCOUNT BALANCE?
YES
NO
C

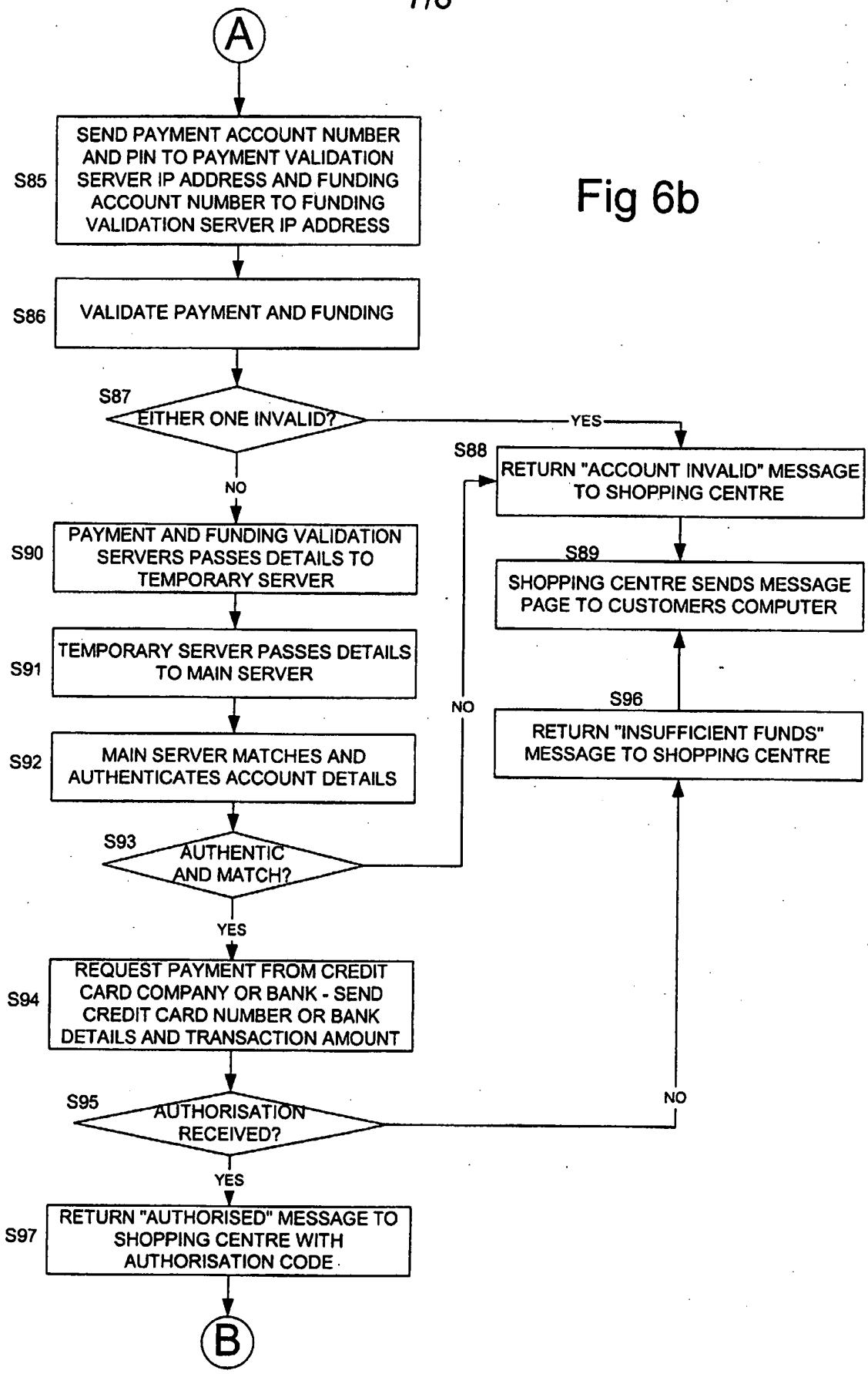

A
S85
SEND PAYMENT ACCOUNT NUMBER AND PIN TO PAYMENT VALIDATION SERVER IP ADDRESS AND FUNDING ACCOUNT NUMBER TO FUNDING VALIDATION SERVER IP ADDRESS
S86
VALIDATE PAYMENT AND FUNDING
S87
EITHER ONE INVALID?
YES
NO
S88
RETURN "ACCOUNT INVALID" MESSAGE TO SHOPPING CENTRE
S89
SHOPPING CENTRE SENDS MESSAGE PAGE TO CUSTOMERS COMPUTER
S90
PAYMENT AND FUNDING VALIDATION SERVERS PASSES DETAILS TO TEMPORARY SERVER
S91
TEMPORARY SERVER PASSES DETAILS TO MAIN SERVER
S92
MAIN SERVER MATCHES AND AUTHENTICATES ACCOUNT DETAILS
S93
AUTHENTIC AND MATCH?
NO
YES
S94
REQUEST PAYMENT FROM CREDIT CARD COMPANY OR BANK - SEND CREDIT CARD NUMBER OR BANK DETAILS AND TRANSACTION AMOUNT
S95
AUTHORISATION RECEIVED?
NO
YES
S96
RETURN "INSUFFICIENT FUNDS" MESSAGE TO SHOPPING CENTRE
S97
RETURN "AUTHORISED" MESSAGE TO SHOPPING CENTRE WITH AUTHORISATION CODE
B

Fig 6b

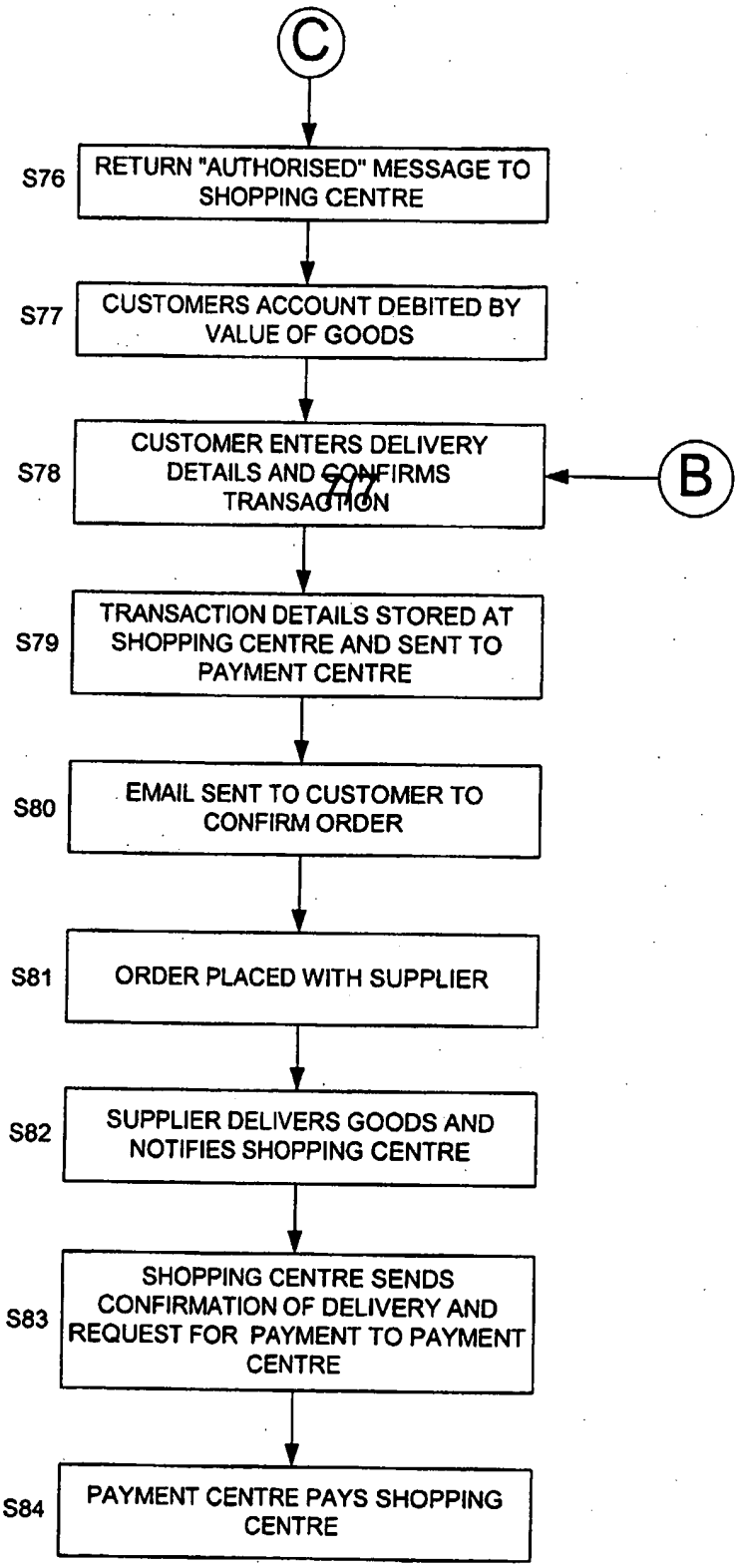

C
S76
RETURN "AUTHORISED" MESSAGE TO SHOPPING CENTRE
S77
CUSTOMERS ACCOUNT DEBITED BY VALUE OF GOODS
S78
CUSTOMER ENTERS DELIVERY DETAILS AND CONFIRMS TRANSACTION
B
S79
TRANSACTION DETAILS STORED AT SHOPPING CENTRE AND SENT TO PAYMENT CENTRE
S80
EMAIL SENT TO CUSTOMER TO CONFIRM ORDER
S81
ORDER PLACED WITH SUPPLIER
S82
SUPPLIER DELIVERS GOODS AND NOTIFIES SHOPPING CENTRE
S83
SHOPPING CENTRE SENDS CONFIRMATION OF DELIVERY AND REQUEST FOR PAYMENT TO PAYMENT CENTRE
S84
PAYMENT CENTRE PAYS SHOPPING CENTRE

Fig 6c

SECURE NETWORK PAYMENT SYSTEM

The present invention generally relates to a system for authorizing payment for goods and services securely over a network such as the Internet. In particular, the present invention relates to the authorization of payment for goods and services by a payment centre holding a customer's account to allow a customer to electronically order goods or services from a server connected to the payment centre by a network such as the Internet.

The safety and convenience of trading on-line plays an important role in the advancement of e-commerce. Normally shopping on-line is built on the relationships among the website offering goods, financial institutions, e.g. banks, credit card issuers, etc., and a user. When trading on-line, the user has to key in his personal and financial information in order to complete the transaction. This is the most dangerous part of trading on-line since the user exposes his information on the Internet.

The present invention provides a solution to the problem of security for electronic commerce by providing a secure payment centre for authenticating electronic transactions. Validation checks take place by using a plurality of validation servers that are individually and irregularly connected to a network to receive requests for authentication of payment information. By irregularly connecting different validation servers for the authentication process, it is difficult for a hacker to break into the payment centre since each validation server is not connected to the network for very long.

Each validation server can include a security module such as a firewall to prevent unauthorized access. Each security module can be different, thereby making it very difficult for a hacker to gain access to the validation servers since each time one is connected to the network, the hacker must start again trying to hack into the validation server.

In one embodiment, the validation servers determine whether the payment information is of valid type e.g. whether the account number and password or PIN are of a valid type. In this embodiment, the payment centre includes a main server for receiving the payment information and information on the value of the goods or services, for authenticating the payment information using information on the customers account, for authorising the order by comparing the information on the value of the goods or services and funds in the customers account, and for sending authorisation information to the supply server in dependence upon the result of the authentication and authorisation. Thus in this embodiment, the customers account can hold funds to be used for payment for goods or services. The funds can be paid into the account using a credit card e.g. by using a telephone to avoid security problems of passing credit card details over the Internet. Funds can also be paid in by direct debit e.g. a fixed amount can be kept in the account by automatically debiting a bank account when necessary. The account at the payment centre (the payment account) is secure because of the use of the plurality of servers that are connected one at a time.

In one embodiment, to increase security, the validation servers are isolated from the main server by a temporary server. The temporary server avoids a direct channel between the validation servers and the main server by disconnecting the validation servers or the main server when a connection is made to the main server or the validation servers respectively.

In an embodiment of the invention, a funding account is set up at the payment centre for accessing funds at a funding institution such as a bank or credit card company. The funding account is assigned an account number and the user selects a password or PIN. Thus when the user selects to pay for the goods or services, they can select to input both the payment account details and the funding account details. Thus the payment information includes information identifying the funding account. A plurality of funding validation servers are provided at the payment centre. Each funding validation server is controlled to connect one at a time for a period of time to the network to

receive the information identifying the funding account and to perform a validation check on the information identifying the funding account. The main server receives any information on the funding account from the funding validation servers, contacts the funding institutions for funding of the order, receives authorisation if funding is authorised by the funding institution, and sends authorisation information to the supply server in dependence upon the received authorisation from the funding institution. This enables a user to select to fund the transaction from another source other that the funds that may or may not be deposited in their account at the payment centre e.g. fund the transaction using credit from their credit card company or bank. The main server is able to access sensitive details such as credit card number using the received funding account details and pass these to the funding institution securely using a secure channel e.g. a dedicated line as is known in the art.

In one embodiment, to increase security, the funding validation servers are isolated from the main server by a temporary server. The temporary server avoids a direct channel between the funding validation servers and the main server by disconnecting the funding validation servers or the main server when a connection is made to the main server or the funding validation servers respectively.

The payment centre of the present invention can be implemented as dedicated electronic hardware. Alternatively, the payment centre can be implemented by any number of general-purpose suitably programmed computers. For example, each of the validation servers can comprise a separate computer. Alternatively, each of the validation servers can comprise a separate server application implemented on a single general-purpose computer.

Since the present invention can be implemented by the software controlling one or more general-purpose computers, the present invention encompasses computer program code for controlling a computer to implement the functionality of the payment centre.

An embodiment of the present invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of a secure payment system in accordance with an embodiment of the present invention;

Figure 2 is a schematic diagram of the payment centre of the embodiment of figure 1;

Figure 3 is a flowchart illustrating the method of setting up a funding account using a credit card over the telephone;

Figure 4 is a flowchart illustrating the method of setting up a funding account using direct debiting instructions to the customer's bank;

Figure 5 is a flowchart illustrating the method of activating a payment account; and

Figures 5a, 5b and 5c are a flow diagram illustrating the method of purchasing goods using the secure payment system.

Referring now to Figure 1, at a customer's premises 1000 a customer has a computer 100 loaded with a web browser 100a for accessing the Internet 400. Also, the customer has a telephone handset 101 connected to the public switch telephone network (PSTN) 200. A payment centre 300 is connected to the Internet 400 and to the public switch telephone network 200. A shopping centre is hosted on a supply server 500 that is connected to the Internet 400. The shopping centre includes the web server 501, an e-mail server 504, a shopping application 502 and a shopping database 503. Within the supply server the web server 501 and the shopping application 502 comprise software applications implemented on a general-purpose computer operating as a server. Thus the shopping centre 500 provides a website which can be visited in order to purchase goods or services.

The payment centre 300 is provided to fund the e-commerce transaction by initially authorizing the transaction and subsequently making payment from funds available from the customer's payment account or by obtaining authorisation for the funding of the transaction from a funding institution such as a bank or credit card company.

A payment centre web host 3000 having a web server 3050 is provided to allow a customer to set up an account with the payment centre 300, view transactions, and authorise topping up of funds in the account. No details are held on the payment centre web host 3000. All details are held securely by the payment centre 300 and are communicated securely between the payment centre 300 and the payment centre web host 3000 over the Internet using the secure socket layer.

The payment centre of this embodiment is illustrated in more detail in Figure 2. Two payment validation servers 310 and 320 are provided. Each payment validation server comprises a respective firewall 311 and 321as a secure interface to the Internet 400. Each payment validation server also comprises a validation application 313 and 323 for interfacing to the Internet and for validating transactions with reference to respective databases 314 and 324 that hold data on valid account numbers and passwords or PINs. The payment validation servers 310 and 320 perform a first level of validation on payment account information by checking to see if the account number and PIN or password is of a valid type.

The payment centre 300 also includes two funding validation servers 330 and 340. Each funding validation server comprises a respective firewall 331 and 341as a secure interface to the Internet 400. Each funding validation server also comprises a validation application 333 and 343 for interfacing to the Internet and for validating transactions with reference to respective databases 334 and 344 that hold data on valid account numbers and passwords or PINs. The funding validation servers 330 and 340 perform a first level of validation on funding account information by checking to see if the account number and PIN or password is of a valid type.

The payment centre 300 also includes a server controller 350 for controlling the payment validation servers 310 and 320 to randomly connect to the Internet 400 one at a time. The server controller 350 also controls the funding validation servers 330 and 340 to randomly connect to the Internet 400 one at a time.

Temporary controllers 360 and 365 are provided as an interface between the funding validation servers 310 and 320 and the payment validation servers 330 and 340 and a main server 370. The main server 370 has a main database 380 which stores customer payment and funding account details including account number, password or PIN, payment account balance, transaction records, personal data and bank or credit card details. A telecommunications interface 390 is provided between the public switch telephone network 200 and the main server 370 within the payment centre 300. This provides the customer with a telephone interface to the payment centre 300 to enable the customer to open an account and enter funds into their account by telephone. There is thus a secure means by which the main server 370 can be accessed by a customer. There is never a channel provided over the Internet to the main server 370 and hence the main database 380.

The method of operation of the secure payment system will now be described with reference to the flow diagrams of Figures 3 to 6.

Figure 3 is a flow diagram illustrating a method by which the main server 370 can be accessed by telephone in order to open an account using a credit card.

In step S1 the customer dials up the payment centre 300 using the telephone handset 101 via the public switch telephone network 200 to the telecommunications interface 390. In step S2 the customer enters their credit card number. In step S3, an authorization check is then performed by the main server 370 using the telecommunications interface 390 to contact a credit card centre or bank 600 via the public switch telephone network 200. In step S4 the customer is then informed whether or not the their credit card has been authorized. If the card has been authorized in step S5, in step S6, the main server

370 generates a funding account number for the customer and this is sent to the customer. In step S7 the customer enters a chosen PIN for the funding account and, in step S8, the funding account is set up by making an entry in the main database 380 which includes the funding account number, the PIN, the customer's credit card details, and other personal details such as name, address, e-mail address, telephone number, etc. The process is then completed in step S9. If in step S5 it is determined that the customer is not authorized, since the customer has been informed in step S4 that the transaction has not been authorized, the process terminates at step S9.

Figure 4 is a flow diagram illustrating a method by which an account can be opened using a direct debit instruction to a bank.

In step S30 the web site hosted by the web host 3000 is accessed by the customer and in step S31 the customer selects to open an account by direct debit. The main server 370 issues the customer with a funding account number that is sent and displayed to the customer in step S32. The customer can then select and enter a funding account PIN in step S33 and, in step S34, a direct debit authorisation form is downloaded. In step S35 the customer prints, completes the form and sends it to the bank to set up the direct debit. In step S36 the bank notifies the payment centre of the direct debit details and in step S35, the funding account is set up by making an entry in the main database 380 which includes the funding account number, the PIN, the customer's bank details, and other personal details such as name, address, e-mail address, telephone number, etc. The process is thus complete (step S38).

Figure 5 is a flow diagram illustrating how the customer's account is activated.

In step S11, the web site hosted by the web host 3000 is accessed by the customer and in step S12 the customer selects to activate an account. In step S13, the customer enters their funding account number and PIN obtained from the process of figures 3 or 4. The details are sent to the payment centre securely over the Internet 400 and are passed to the main server 370 by the validation servers 310, 320, 330 and 340 and the temporary

servers 360 and 365. A validation check is carried out in the main server 370 using the main database 380 to compare the input data with the stored data. If the input account number and PIN are invalid, in step S15 a notice is generated and sent to the web host 3000 which generates a notice as part of a web page which is sent to the customer's computer 1000 to inform them that the account is invalid. If the account number and PIN are valid, in step S16 the customer will enter personal details that will be entered in the main database 380 by the main server 370. In step S17, the customer can then select whether or not to use the auto top-up facility. This enables the payment centre to always keep a fixed amount in the customers payment account by taking funds from their credit card or bank in dependence upon the way the customer has set up their funding account. If auto top-up is selected, in step S18, the customer enters the amount to be kept in their payment account. The main server 370 then, in step S19 generates a payment account number for the customer and sends it to the customers computer for display as part of a web page. The customer then (step S20) enters a PIN number to be used for the payment account into their computer and this is sent to the main server 370 and in step S21 the database entry for the customer is updated to include the payment account number and selected PIN. The customer's account is then activated and the process is complete (step S22).

Thus, using this method, a customer is able to deposit funds in an account stored in the main database 380 within the payment centre 300. The funds are thus available for electronic transactions made over the Internet 400 with shopping centres 500 by customers using customers' computers 100. They are able to access their account using both account numbers and passwords to manually top up the funds in their payment account by instructing a transfer of funds from their credit card account or bank account. This can be done over the Internet securely because both account numbers and PINs are required. These are sent the respective validation servers over separate channels using different IP addresses. The web host 3000 provides the web interface for the top up feature by securely communicating with the validation servers 310, 320, 330 and 340 and hence the main server 370. The web host 3000 also enables a customer to view a

transaction history for their account by virtue of the secure communications with the main server 370.

The method of carrying out the electronic transactions will now be described with reference to the flow diagram of Figures 6a to 6c

In step S60, a customer uses the customer's computer 100 to point the web browser 100a to access the website hosted by the web server 501 at the shopping centre 500. A customer uses the web browser 100a to navigate through the website hosted by the web server 501 to choose goods to be purchased. The customer selects the secure method of payment as an option available on the payment page of the website and in step S61 a web page is displayed enabling the customer to enter both their payment and funding account numbers and PINs. The entered account numbers and PINs are sent from the customer's computer 100 to the shopping centre 500 and are received by the web server 501. The shopping application 502 extracts the account numbers and PINs and then instructs the web server 501 to send the account numbers, PINs and information on the value of the goods being purchased to the payment centre 300 in step S62. This information can be sent as part of a HTML request to a web server in the payment centre 300. If only the payment account number and PIN have been entered by the customer (step S63), the payment account number and PIN are sent to the IP address of the payment validation server 310 or 320 (step S64). The payment validation server 310 or 320 that is connected to the Internet checks to determine if the account number and PIN are of valid type (step S65). In step S66 if the numbers are invalid, in step S67 an "account invalid" message is generated and returned to the shopping centre 500. The shopping centre 500 then generates and sends a message web page to the customers computer 1000 to inform the customer in step S68. If on the other hand the numbers are valid (step S66), in step S69 the payment validation server 310 or 320 passes the account number, PIN and value of the transaction to the temporary server 365. The temporary server 365 then passes the data onto the main server 370 in step S70. The main server 370 then performs an authentication of the account number and PIN using the customer data stored in the main database 380. If the numbers are not authenticated

(step S72), in step S67 an "account invalid" message is generated and returned to the shopping centre 500. The shopping centre 500 then generates and sends a message web page to the customer's computer 1000 to inform the customer. If on the other hand the numbers are authenticated (step S72), in step S73 the value of the goods or services in the transaction are checked against the funds in the customers payment account. If the value of the transaction exceeds the funds (step S74), in step S75 an "insufficient funds" message is generated and returned to the shopping centre 500. The shopping centre 500 then generates and sends a message web page to the customer's computer 1000 to inform the customer in step S68.

If in step S74 it is determined that the value of goods does not exceed the current balance in the customer's account, in step S76 the payment centre returns a message indicating that the transaction is authorized to the shopping centre 500. In step S77 the customer's account is then debited by the value of the goods in the payment centre 300. In step S78, having received the authorization, the shopping application generates a web page to enable the customer to enter delivery details and to confirm the transaction. The transaction details are then stored at the shopping centre in step S79 and also sent to the payment centre 300. An email is then sent to the customer by the email server 504 within the shopping centre 500 in order to confirm the order (step S80). An order can then be placed by email with the supplier in step S81 and in step S82 the supplier then delivers the goods and notifies the shopping centre by email. The shopping centre then sends confirmation of delivery and requests the payment in step S83 to the payment centre 300. In step S84 the payment centre then makes payment to the shopping centre 500 to complete the transaction.

If in step S63 both the payment and funding account numbers are entered by the customer, in step S85 the payment account number and PIN are sent to the payment validation server 310 or 320 and the funding account number and PIN are sent to the funding validation server 330 or 340. In step S86 the servers check to determine if the payment account number and Pin and the funding account number and PIN are of a valid type. If not (step S87), in step S88 an "account invalid" message is generated and

returned to the shopping centre 500. The shopping centre 500 then generates and sends a message web page to the customers computer 1000 to inform the customer in step S89. If on the other hand the numbers are of valid type (step S87), in step S90 the payment validation server 310 or 320 passes the payment account number and PIN and the transaction amount to the temporary server 365 and the funding validation server 330 or 340 passes the funding account number and PIN to the temporary server 360. The temporary servers 360 and 365 then pass the data on to the main server 370 (step S91. In step S92 the main server then performs an authentication and matching of the account numbers and PINs to the data stored in the main database 380. If this fails (step S93), in step S96 an "account invalid" message is generated and returned to the shopping centre 500. The shopping centre 500 then generates and sends a message web page to the customers computer 1000 to inform the customer in step S89.

If the account numbers are authentic and match (step S93), in step S94 the main server generates a request for payment from the credit card centre or bank 600. The request includes the credit card number or bank details and details of the amount of the transaction. In step S95 authorisation for the funding of the transaction is awaited. If authorisation is not given, in step S96 an "insufficient funds" message is generated and returned to the shopping centre 500. The shopping centre 500 then generates and sends a message web page to the customers computer 1000 to inform the customer in step S89. If authorisation is given (step S95), in step S97 the payment centre returns a message indicating that the transaction is authorized to the shopping centre 500.

Thus using this method a customer can select to pay using funds available in their payment account at the payment centre by only entering their payment account details. If they wish to fund the transaction using funds in a bank or by seeking credit e.g. from a credit card company, the funding account details must also be entered. This increase security since the considerably larger funds available to the customer from the funding institution is only accessible with both sets of details. (The more limited funds in the payment account can be accessed using just the one set of details.) This use of two sets

of details together with the use of the multiple access servers 310 and 320, and 330 and 340, provide a secure payment system.

In one embodiment each of the authentication servers can connect to the Internet using a different Internet address. Thus in this embodiment, order for the shopping centre 500 to be able to connect to the connected authentication server within the payment centre 300, it must be informed of the IP address to which it must direct its queries for authentication of transactions.

Although the present invention has been described hereinabove with reference to a specific embodiment, it will be apparent to the skilled person in the art that modifications can be made which lie within the spirit and scope of the present invention.

For example, the payment centre can be implemented using hardware or software implemented on one or more general purpose computers.

Further, although the embodiment describes the use of customer accounts having funds, the present invention is equally applicable to a credit service.

CLAIMS:

1. A payment method over a network comprising:

setting up a customer account at a payment centre;

accessing a supply server;

receiving a customer order for goods or services at the supply server, the customer order comprising payment information identifying the customer account at the payment centre;

at the supply server, transmitting over the network the payment information and information on the value of the goods or services to the payment centre;

at the payment centre, using the payment information to perform a validation check on the customer order by accessing data on the customer's account and responding by sending validation information to the supply server; and

at the supply server, responding to the validation information to process the customer order accordingly;

wherein at the payment centre a plurality of validation servers are provided, each validation server being controlled to connect one at a time for a period of time to the network to receive the payment information, to perform a validation check, and to send the authorisation information to the supply server.

2. A payment method according to claim 1, wherein the validation servers are each controlled to connect irregularly to the network.

3. A payment method according to claim 1 or claim 2, wherein each validation server includes a security module to prevent unauthorized access, and when information is passed to the respective validation server it is security checked by the security module.

4. A payment method according to claim 3, wherein each security module performs a different type of security checking procedure.

5. A payment method according to any preceding claim, wherein the validation servers determine whether the payment information is of valid type, the payment centre includes a main server for receiving the payment information and information on the value of the goods or services, for authenticating the payment information using information on the customers account, for authorising the order by comparing the information on the value of the goods or services and funds in the customers account, and for sending authorisation information to the supply server in dependence upon the result of the authentication and authorisation.

6. A payment method according to claim 5, wherein the main server is isolated from the validation servers by a temporary server.

7. A payment method according to claim 5, including setting up a funding account at the payment centre for accessing funds at a funding institution, and wherein the payment information can include information identifying the funding account, a plurality of funding validation servers are provided at the payment centre, each funding validation server being controlled to connect one at a time for a period of time to the network to receive the information identifying the funding account and to perform a validation check on the information identifying the funding account.

8. A payment method according to claim 7, wherein the main server receives any information on the funding account from the funding validation servers, contacts the funding institutions for funding of the order, receives authorisation if funding is authorised by the funding institution, and sends authorisation information to the supply server in dependence upon the received authorisation from the funding institution.

9. A payment method according to claim 8, wherein the main server is isolated from the funding validation servers by a temporary server.

10. A payment method according to claim 5, wherein the main server includes a database of customer account information.

11. A payment method according to any preceding claim, wherein the funds are supplied to the customer's account by telephone instructions.

12. A payment method according to any preceding claim, wherein the payment information includes the customer's account number and a password.

13. A payment centre apparatus for connection to a network to validate and authorize payment, the apparatus comprising:

a plurality of servers for receiving payment information identifying a customer account over the network from a supply server and for transmitting authorisation information over the network to the supply server;

authorising means for using the payment information to perform an authorisation check to generate the authorisation information; and

controlling means for controlling the servers to connect to the network one at a time for predetermined periods of time.

14. A payment centre apparatus according to claim 13, wherein said controlling means is adapted to control the servers to connect irregularly to the network.

15. A payment centre apparatus according to claim 13 or claim 14, wherein each server includes a security module for preventing unauthorized access by security checking received information.

16. A payment centre apparatus according to claim 15, wherein each security module is adapted to perform a different type of security checking procedure.

17. A payment centre apparatus according to any one of claims 13 to 17, wherein the servers comprise validation servers adapted to determine whether the payment information is of a valid type, the authorising means comprises a main server for receiving the payment information on the value of the goods or services, for

authenticating the payment information using information on the customers account, for authorising the order by comparing the information on the value of the goods or services and funds in the customers account, and for sending authorisation information to the supply server in dependence upon the result of the authentication and authorisation.

18. A payment centre apparatus according to any one of claim 17, including a temporary server, wherein the main server is isolated from the servers by the temporary server.

19. A payment centre apparatus according to claim 17, wherein a funding account is set up at the payment centre for accessing funds at a funding institution, and the payment information can include information identifying the funding account, the apparatus including a plurality of funding validation server, each funding validation server being controlled to connect one at a time for a period of time to the network to receive the information identifying the funding account and to perform a validation check on the information identifying the funding account.

20. A payment centre apparatus according to claim 19, wherein the main server is adapted to receive any information on the funding account from the funding validation servers, to contact the funding institutions for funding of the order, to receive authorisation if funding is authorised by the funding institution, and to send authorisation information to the supply server in dependence upon the received authorisation from the funding institution.

21. A payment centre apparatus according to claim 20, including a temporary server, wherein the main server is isolated from the funding validation servers by the temporary server.

22. A payment centre apparatus according to claim 17, wherein the main server includes a database of customer account information.

23. A payment centre apparatus according to any one of claims 13 to 22, including a telecommunications interface allowing funds to be transferred to the customer's account.

24. A payment centre apparatus according to claim 17, wherein said payment information includes an account number and a password, and said main server is adapted to perform the authentication by comparing the received account number and password with the account number and password in stored data.

25. A payment centre apparatus according to claim 20, wherein said information on the funding account includes an account number and a password, and said main server is adapted to perform the authentication by comparing the received account number and password with the account number and password in stored data.

26. A payment centre apparatus according to claim 24 and claim 25, wherein said main server is adapted to match the account numbers and password to determine if they belong to the same customer and to generate the authorisation information in dependence upon the outcome of the matching process.

INVESTOR IN PEOPLE

Application No: GB 0101864.7
Claims searched: 1-26

Examiner: Paul Marshall
Date of search: 22 November 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4A (AAP, AUDB, AUXF, AUXX)

Int Cl (Ed.7): G06F 1/00, 17/60

Other: Online: EPODOC, WPI, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
-	None	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.